REMARKS

This Amendment is in response to the Non-Final Office Action dated April 30, 2008.

Claims 1-14, 16, 18 and 20-23 were rejected under 35 U.S.C. 103(a) as being unpatentable over Tripunitara et al. (U.S. Patent No. 6,771,649 B1), in view of what was well known in the art at the time of the invention, and further in view of Razzaghe-Ashrafi et al. (U.S. Patent No. 6,202,169 B1).

For the purposes of the file history, Applicant respectfully submits that the stated rationale for the 35 USC 103 rejeetion is flawed. While the Examiner argues that it was known in the prior at to include the function of a firewall on a host computer, it is respectfully submitted that the Examiner has missed an essential point. The prior art does not teach or suggest that a single firewall resident on a host computer can be used to protect against an ARP attack. Tripunitara provides protection at a gate. Razzaghe deals with the entirely unrelated problem of transitioning to a redundant computer on a network. The references cannot be properly combined to achieve Applicant's claimed invention.

Nevertheless, in the interests of better explaining to the Examiner how a single firewall resident on a host computer protects against ARP attacks Applicants have amended the independent claims to clarify how the claimed invention deals with both genuine address resolutions and spoofed address resolutions. Support for this amendment is found in Figures 6-7 and paragraphs [0032]-[0034].

In particular, Applicants have amended claim 1 to better illustrate how ARP spoofing attacks are distinguished from genuine address resolution message. Figure 6 illustrates the case where a target computer station issues an unsolicited message that submits a genuine address resolution. In this situation, when the host attempts to authenticate the message by issuing a broadcast message for network elements to respond with address resolution information, it will not receive any messages that submit the previously cached address resolution. That is, it will not receive any reply messages that contradict the genuine address resolution that was submitted. In fact, the target will respond back with the genuine address resolution. Consequently, the message was not spoofed. Figure 7 illustrates the case where the spoofer submits a spoofed address resolution. In this case, when the host attempts to authenticate the message it will receive a reply message from the target computer station that has the previously cached address resolution. Thus, there is a contradiction which demonstrates that the spoofed address resolution can't be correct. That is, the fact that the target computer replies back with the previously cached addrcss resolution is logically incompatible with the spoofers's unsolicited address resolution. Consequently, the firewall recognizes that there was an attempted spoofing attack and blocks an update of the cached address resolution information.

The other independent claims were also amended to clarify how spoofed messages are distinguished from genuine address resolution messages.

It is respectfully submitted that the amended claims distinguish over the prior art. None of the cited art, alone or in combination, teaches all of the elements of the amended claims. Moreover, the cited art does not teach or suggest the functionality of the claimed invention.

It is respectfully submitted that all of the pending claims are in condition for allowance. If there are any other residual formalities that need to be resolved prior to allowing the subject application, the Examiner is requested to contact the undersigned.

The Commissioner is hereby authorized to charge any appropriate fees to Deposit Account No. 50-1283.

Respectfully submitted,
COOLEY GODWARD KRONISH LLP

Dated: 6/5/2008

By: Edward Van Gieson

Edward Van Gieson
Reg. No. 44,386

COOLEY GODWARD KRONISH LLP
ATTN: Patent Group
Five Palo Alto Square
3000 El Camino Real
Palo Alto, CA 94306-2155
Tel: (650) 843-5625
Fax: (650) 857-0663

EVG:dlh